TP CYBER :

Dans ce TP, nous allons installer le nécessaire pour faire fonctionner une application web. Pour cela, nous installerons un serveur Apache HTTPD, une base de données MariaDB (anciennement MySQL) et le langage de programmation PHP. Ces installations se feront sur une machine virtuelle utilisant le SE Rocky Linux (anciennement CentOS).

Utilisation Nmap :

|  |
| --- |
| Pour tester la version de l’ OS et tester les ports :  sudo nmap ADRESSE\_IP\_ROCKY\_LINUX -O -sV -p1-65535  Résultat : |
| Iptables -L  Ma configuration : |
|  |
|  |

Sur Kali, décompressez l'archive de mots de passe *rockyou* qui se trouve dans le répertoire */usr/share/wordlists*

hydra -L bruteforce.txt -P rockyou.txt 192.168.56.152 ssh -t 4

|  |
| --- |
|  |

Installation d’apache :

|  |
| --- |
| etc/httpd |

Configuration pare-feu pour autoriser a accéder au site web depuis l’extérieur.

|  |
| --- |
| Iptables -I INPUT -p tcp –dport 80 -j ACCEPT |
| Nikto sert à lister des failles de sécurité  Nikto -h addresse ip server    Pour éviter ces failles on peut modifier les fichiers de conf d’apache :  /etc/apache2/sites-available/000-default.conf :    Fichier secur.conf : |

Une fois php installé sa version est visible pour corriger ce probleme :

|  |
| --- |
| Vi /etc/php.ini Expose\_php = off |

En conclusion :

Ce TP permet de vérifier le respect des règles d’utilisation des ressources numériques en améliorant la cybersécurité du server web apache. Il permet aussi de travailler en projet notamment pour trouver les correctifs a mettre en place pour corriger les problèmes de sécurités découvert grâce à nikto.